JOURNAL OF FORENSIC SCIENCES

J Forensic Sci, November 2009, Vol. 54, No. 6
doi: 10.1111/j.1556-4029.2009.01150.x
Available online at: interscience.wiley.com

Eoghan Casey,[1] *M.A.; Monique Ferraro,*[2] *J.D., M.S.; and Lam Nguyen,*[3] *M.Inf.Tech.*

Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence*

ABSTRACT: There is an urgent need to reduce the growing backlog of forensic examinations in Digital Forensics Laboratories (DFLs). Currently, DFLs routinely create forensic duplicates and perform in-depth forensic examinations of all submitted media. This approach is rapidly becoming untenable as more cases involve increasing quantities of digital evidence. A more efficient and effective three-tiered strategy for performing forensic examinations will enable DFLs to produce useful results in a timely manner at different phases of an investigation, and will reduce unnecessary expenditure of resources on less serious matters. The three levels of forensic examination are described along with practical examples and suitable tools. Realizing that this is not simply a technical problem, we address the need to update training and establish thresholds in DFLs. Threshold considerations include the likelihood of missing exculpatory evidence and seriousness of the offense. We conclude with the implications of scaling forensic examinations to the investigation.

KEYWORDS: forensic science, digital forensics, digital evidence, forensic best practices, laboratory management, triage forensic inspection, survey forensic examination, in-depth forensic examination, ethical considerations

The increasing capacity of commonly used storage media, large amounts of data on networks, expanding variety of computing devices, growing case loads, and limited resources are combining to create a crisis for Digital Forensics Laboratories (DFLs). Despite their best efforts to keep up with the growing case load and increasing amounts of data, many DFLs have backlogs of 6 months to 1 year. Such delays in processing evidence are harmful and will inevitably bog down the criminal justice system, giving offenders time to commit additional crimes and causing immeasurable damage to falsely accused individuals.

As these trends unfold, few DFLs can still afford to create a forensic duplicate of every piece of media and perform an in-depth forensic examination of all data on those media. Keep in mind that attempting to examine "everything" can cause data overload that can lead to hasty processing, which can result in mistakes that compromise an investigation. On the other hand, not examining the most pertinent evidence in an expedient manner may result in incomplete investigations or completely missed leads. There is a need for a more manageable and effective approach to performing forensic examinations to better support safety and justice.

Previously proposed solutions to dealing with these challenges concentrate on selective preservation of evidence (1). The ACPO Good Practice Guide for Computer-Based Electronic Evidence, which formerly promoted forensic duplication, has been updated to accommodate situations when it is not viable to preserve all available data, stating that "partial or selective file copying may be considered as an alternative" to making a full forensic duplicate and (2) although selective preservation has its place, it has serious limitations and must be considered in a broader context. Before evidence is excluded from a forensic examination, more fundamental decisions must be made regarding thresholds of when such time saving measures are appropriate. The process of establishing thresholds is specific to each DFL, and can include rating the seriousness of the offense, case circumstances and type of evidence sought, likelihood of missing exculpatory evidence, and the importance of other data on the storage media.

From our collective experience as forensic practitioners, we have noted trends and have seen how cases tend to develop and resolve. It makes little sense to wait for the review of each piece of media if only a handful of them will provide data of evidentiary significance. At this point, there are enough examples to justify a new approach to case management which involves tailoring forensic examination of digital evidence to the type of crime or case under investigation. Specifically, three levels of forensic examination are defined to deal with the most common situations that arise:

- Survey/triage forensic inspection: Targeted review of all available media to determine which items contain the most useful evidence and require additional processing.
- Preliminary forensic examination: Forensic examination of items identified during survey/triage as containing the most useful evidence, with the goal of quickly providing investigators with information that will aide them in conducting interviews and developing leads.
- In-depth forensic examination: Comprehensive forensic examination of items that require more extensive investigation to gain a more complete understanding of the offense and address specific questions.

These three levels of forensic examination extend existing process models for conducting digital investigations that promote the forensic duplication and in-depth forensic examination of all media (3,4). In addition, this tiered strategy takes into account the Computer Forensics Field Triage Process Model (CFFTPM) for

[1] Johns Hopkins University, Information Security Institute, Wyman Park Building, 3400 North Charles Street, Baltimore, MD.

[2] Technology Forensics, LLC, Waterbury, CT.

[3] Stroz Friedberg, LLC, Boston, MA.

*A portion of this work presented at the High Technology Crime Investigation Association International Conference in Washington, DC, September 2004.

Received 26 June 2008; and in revised form 17 Sept. 2008; accepted 13 Nov. 2008.

conducting triage forensic inspections in the field when investigators require immediate results (5). Each level of examination listed above can be performed either in the field or in the laboratory, with DFLs making this decision based on the specific case and available resources.

In some circumstances it is necessary to perform a survey/triage forensic inspection of all available items prior to examining particular items in more depth. For instance, when criminal activity originated from an organization or Internet café with hundreds of computers, it may be necessary to perform a survey/triage forensic inspection of each computer to identify those that may have been involved in the crime. In other circumstances it is more effective to focus on a few items initially, before performing a survey/triage forensic inspection of all available media. For example, in a child exploitation case involving several computers and a large amount of removable media, it can be most effective to perform survey/triage forensic inspections of the computers (because they generally contain the most information about user activities), then a preliminary forensic examination of the most relevant computer, and subsequently process the remaining items as needed. When a cellular telephone or other device containing volatile data is a potential source of evidence, performing a survey/triage forensic inspection immediately can reveal valuable information that may not be available later. Under certain circumstances, it may also be necessary to examine the network on which a computer resides to determine whether analysis of additional computers, logs, and other related data is required (6).

This is not to say that existing methods are invalid, or that in-depth forensic examinations be curtailed for the sake of expediency. There are definitely situations in which an in-depth forensic examination is still necessary, particularly when a case goes to trial.

This tiered strategy for conducting forensic examinations is based on the observation that certain cases require significant time and resources whereas other cases can be expedited, saving valuable resources. The goal of this approach is to maximize the amount of time forensic examiners spend producing results that are directly relevant to the case at hand. In fact, many forensic examiners already make these decisions, informally expediting the process based on their best judgment of the needs in each case. However, this decision-making process is not formalized in current DFL policies and protocols, and the absence of policies and protocols for such activities can lead to inconsistencies in how cases are handled, creating problems for DFLs and forensic examiners.

These three levels of forensic examinations are designed to be applicable in any DFL setting, whatever the focus and type of case work. We define evidence broadly to include facts that will be put into evidence during legal cause of action as well as information that leads to the discovery of evidence, often referred to as intelligence. Although we concentrate on the handling of storage media in DFLs this tiered approach can be applied to other forms of evidence, including mobile phones, global positioning system (GPS) navigation systems, and other digital devices. Furthermore, although our focus is on criminal investigations, this tiered approach has relevance to electronic data discovery, as well as border security checks and customs searches for contraband on computers. With regard to discovery in civil litigation, timely analysis of electronically stored information is critical in order to develop an efficient discovery plan and investigative strategy, while lengthy delays can have financial ramifications for civil defendants.

The Background section provides background of the challenges that DFLs currently face and the implications of resulting delays. Materials and Methods describes the tiered forensic examination process, covering relevant tools and techniques. The Discussion section discusses implementation considerations of the tiered strategy and applying thresholds in DFLs to prioritize cases and allocate resources. The Conclusion section concludes this paper.

Background

Current best practice guidelines focus on forensic duplication of storage media (4,7) which is too time-consuming and costly for many situations encountered during modern digital investigations. In just the past few years, storage has increased on typical hard drives from hundreds of megabytes to hundreds of gigabytes. In terms of pages of text, a 200 GB drive can store *c.* 52,000,000 pages of text or about 4,000,000 digital images. A common child pornography investigation may yield hundreds or thousands of pieces of media including hard drives, flash thumb drives, and optical media that make it infeasible to create forensic duplicates of every item. In one media piracy case, a suspect's house yielded over 40,000 counterfeit and pirated CDs (8). Considering each piece of media in a case as a separate digital crime scene helps further convey the scale of the problem: "the investigation of billions of bytes of digital data is similar to the investigation of a house where an investigator must look at thousands of objects, fibers, and surface areas and use his expertise to identify potential evidence" (9). As DFLs receive increasing quantities of digital evidence, the practice of creating a forensic duplicate and performing an in-depth forensic examination of every item is causing harmful delays.

In a recent case, a sixth grade teacher was accused by a student of viewing pornographic images on a computer in the classroom (10). The teacher denied the charge. He was in the process of writing a musical and was downloading a picture of Jacqueline Onassis, the subject of his work. School officials seized the computer and reported the incident to the local police, who obtained a search warrant and transported the computer to the state DFL for analysis. In the meantime, the school system placed the teacher on administrative leave. Parents and colleagues would come up to the teacher and ask him if he had been arrested. When he saw students, they would call him a "pervert." From the time of the accusation until a "preliminary" verbal report from the DFL exonerating him, nearly 12 months had elapsed. The DFL determined that indeed, the picture he downloaded was that of Jacqueline Onassis. In the interim, the accusation of one single sixth grader seriously impugned the reputation of the more than 20-year teacher and composer. The school system changed his teaching assignment, but he still lives under the cloud of suspicion, bearing the brunt of gossip and innuendo of students, parents, and school administrators.

The current approach to processing digital evidence is particularly problematic when precious resources within DFLs are being squandered on unnecessary tasks. In one sexual assault investigation where there was a significant amount of physical evidence, investigators wanted to know if there was any related evidence on the suspect's computers. It took the DFL 3 weeks to forensically duplicate all of the media only to find that there were just a few relevant pictures. Everyone would have been better served by a preliminary forensic examination of the original evidence using a read-only method and a quick selective preservation and production of the small amount of relevant evidence without ever creating forensic duplicates of the media. In another case, the defense requested a copy of the incriminating files. The files were provided a year after the defendant was arrested and approximately 1 month before the defendant's trial date.

Some DFLs have responded to the work overload and associated delays by implementing a rigid request procedure that requires investigators to specify what they want from the media. In response, forensic examiners only produce what is requested. This approach may increase efficiency in the DFL, and enables them to develop impressive metrics on the number of examinations performed, but investigators are finding that they must submit multiple requests to obtain the digital evidence they need. This approach simply transfers the responsibility for delays in processing digital evidence from DFLs onto investigators, and does not resolve the problem of harmful delays. Additionally, many investigators do not have the requisite technical knowledge to identify the pertinent points of digital evidence that may relate to their case. Investigators often rely on the forensic examiner to identify, interpret, and analyze digital evidence that they may not even realize exists.

In many cases, the greatest utility of digital evidence is at the beginning of an investigation, and that makes the need for fast turnover by DFLs compelling. Locating time-sensitive evidence can enable investigators to prevent harm, such as in school shootings, bomb threats, and the sexual abuse of children. The lack of timely results also puts investigators at a disadvantage when interviewing suspects. Without a clear understanding of the digital evidence and suspect's computer usage, it is more difficult to develop an effective interview strategy. Having overwhelming evidence may help investigators obtain confessions during initial suspect interviews. Delays give offenders time to regain their composure after they are apprehended, and to cover their electronic tracks, potentially reducing the chances of an early confession or negotiated resolution. Some investigators indicate that they feel less inclined to consider computer systems in new cases because of the delays that processing the digital evidence will create in their case. Allowing investigators to work on cases without the help of available digital evidence reduces their chances of resolving the matter successfully.

Delays in processing media can also result in lost opportunities to obtain related digital evidence from other sources, such as network logs from Internet servers. Although proposed legislation seeks to compel Internet Service Providers (ISPs) to retain logs of various kinds, most Internet and network servers do not currently maintain such log data for extended periods of time. The short turnaround is intentional because there is little advantage to the users or administrators to hold on to the data, but various benefits to sloughing off unnecessary and bulky records. In one case, an Indiana man was served with a search warrant after federal investigators determined that he was trading child pornography using a file server over an Internet Relay Chat (IRC) channel. Forensic examination of his computer revealed file transfer logs that could have been used to track down thousands of additional offenders who traded images of hardcore child pornography with the target. Unfortunately, because the computer sat in the DFL for over 3 months before being examined, the age of the file transfer logs rendered them useless because the corresponding ISP logs needed to identify additional offenders were no longer available.

Such lengthy delays in processing evidence are detrimental to defendants, investigative agencies, and the criminal justice system as a whole. One issue of concern in the United States is the right of the accused to a speedy trial as defined by the Sixth Amendment. Six months to a year is probably too long to wait for a forensic examination, especially if the accused cannot make bail and is awaiting trial. There is already a precedent for the exclusion of evidence based on these delays. In *U.S. v. Brunette* (11), a magistrate judge added language to the search warrant directing agents to complete their review of seized computers within 30 days. The review of a second computer did not begin until day 32. In this possession of child pornography case, the court found that the government offered no legitimate reason for the delay, and suppressed evidence from the second computer. Although courts are making an effort to reduce delays, exceptions are made, such as in *U.S. v. Hernandez* (12) where the forensic examination was conducted 5 weeks after the expiration of the search warrant, but the evidence was accepted.

So far, the courts have been fairly lenient with law enforcement agencies for excessive delays between issuance of the search warrant and the examination of electronic evidence. However, the cases so far have addressed delays of a few weeks or months, not years. Furthermore, in jurisdictions in which there is a time frame either stated in the warrant or mandated by statute, challenges to the timeliness of the examination are inevitable (13,14).

Although difficult to quantify, there is also a cost to suspects and victims associated with having their computers and storage media in the custody of a DFL for extended periods of time. In the current paradigm, the DFL could retain possession of computers, peripherals, and storage media for such an extended time that the property loses its value to the owner, either through obsolescence or loss of data.

Materials and Methods

This section describes existing and emerging approaches that offer alternatives to creating full forensic duplicates and performing in-depth forensic examinations of every piece of media. The main rationale for creating a forensic duplicate is to preserve the original evidence from inadvertent alteration. This concern is significantly lessened by improvements in write-blocking technology and the existence of strong verification methods, such as cryptographic hashing functions, used to ensure that digital evidence has not been altered. Forensic boot disks enable forensic examiners to boot a computer and preview its contents without making any alterations to data on the hard drive. In addition, reliable hardware write-block devices connect a hard drive to a forensic workstation in a read-only preview mode, allowing forensic examiners the ability to directly preview data without requiring the lengthy duplication process.

Another concern with reviewing original evidence is that repeated use of the original can result in hardware damage. This risk can be mitigated by creating forensic duplicates of items which have been previewed and ultimately deemed to be of evidentiary significance requiring more extensive examination. Whether or not a forensic duplicate is created, prior to performing any operations on an item of evidence, it should have been documented in accordance with best practices in order to distinguish each item uniquely and to maintain chain of custody throughout the investigation.

It is important to realize that this is not purely a technical issue—the most significant obstacles to changing current practices are DFL policies and expectations of investigators and attorneys. Attorneys, judges, and laboratory administrators must realize that resources devoted to DFLs do not allow for in-depth forensic examination of every item of evidence related to every crime that has a digital nexus. Further, they must realize that forensic duplication and examination of all media is not always necessary. In fact, better results can often be achieved by defining thresholds and intelligently allocating resources based on the specific requirements of a case. Before the new techniques and tools described in this section can be implemented, DFLs must collectively update their current operating procedures with guidelines for scaling examinations to the investigation. Furthermore, attorneys must allow DFLs reasonable flexibility in this regard.

A major part of the overall paradigm shift towards improving the way digital evidence is handled in DFLs is ensuring that forensic examiners, investigators, attorneys, and other relevant parties understand their roles in the overall process. While it is not our intention to redefine individual responsibilities, it is necessary to underscore the need for these individuals to be trained to use digital evidence more effectively. As DFLs adopt a tiered approach to performing forensic examinations, it is important that the changes in procedure be accompanied by training to ensure that all tools and methods are implemented correctly. Breaking forensic examination into tiers simplifies training, making it easier to teach the discrete knowledge and skills required at each level. However, in addition to receiving training in their areas of specialization, all involved parties need an overall understanding of the full life cycle of a case involving digital evidence to ensure they can work in concert to construct a timely and cohesive investigation. Investigators must be able to recognize the significance of certain types of digital evidence before they can be expected to ask forensic examiners to extract that information. Similarly, forensic examiners need an understanding of the law before determining what evidence will meet a prosecutor's burden. And lastly, prosecutors must be able to understand how digital evidence can be used to create a case that is beyond reproach.

Survey/Triage Forensic Inspection

The first level of examination is a survey/triage forensic inspection that involves the rapid review of many potential sources of digital evidence for specific information, with the goal of quickly identifying those items that contain relevant evidence. This process of effectively separating the wheat from the chaff has been alternately referred to as survey and triage. Beebe and Clark describe the survey process as "mapping" the overall "landscape" of the digital evidence to locate "obvious and potential evidence" (15). Carrier draws an analogy between the survey process and an investigator walking "around the crime scene to identify obvious pieces of evidence and pieces of evidence that are transient" (4). Triage of computers as evidence has been described as "a process in which things are ranked in terms of importance or priority" (5). Rogers et al. present triage purely in the context of time critical cases that require evidence to be examined on scene. However, this triage process can be applied to any investigation involving computers, including those of a less time critical nature, and can be performed in the laboratory environment.

Based on the results of the survey/triage forensic inspection process, forensic examiners can focus on the most pertinent sources of evidence and waste less time examining irrelevant computer systems. For instance, a survey/triage forensic inspection can reveal when a hard drive has been completely wiped, avoiding the wasted effort in creating a forensic duplicate of an empty hard drive.

When hundreds of computer systems or large servers are involved, previewing each of them in read-only mode and performing a search for a short list of pertinent keywords or certain types of files can quickly narrow the focus of the investigation to those few systems that contain useful digital evidence. For instance, in cases involving high capacity RAID servers, it can take days to create forensic duplicates of the systems and weeks to sift through millions of keyword hits. Before expending limited resources on an in-depth forensic examination of such large systems, a survey/triage forensic inspection of all available media in read-only mode can help identify the richest sources of evidence, perhaps revealing that a smaller, seemingly less significant system contains the most useful digital evidence.

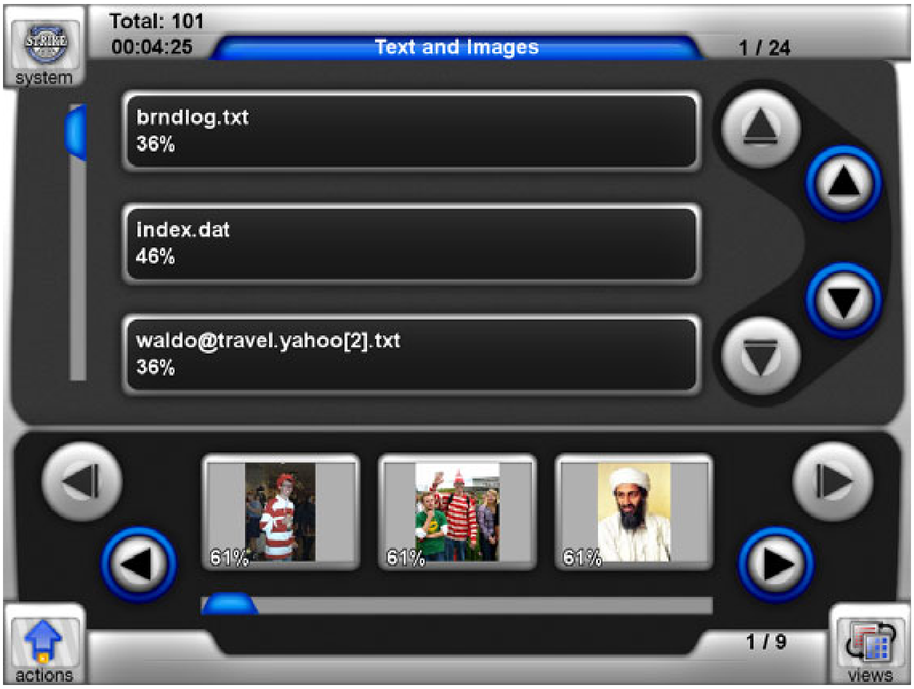
Forensic tools are being developed specifically to perform this type of survey/triage forensic inspection. Some forensic boot disks can be configured with a keyword list and hash sets, allowing forensic examiners to quickly boot and search computers in read-only mode to identify a few computers out of hundreds that contain potentially relevant data. The FBI uses a preview tool called ImageScan to review all graphics files on a computer quickly without altering the original evidence. The Ontario Provincial Police developed a tool called C4P for a similar purpose (http://www.e-crime.on.ca). Triage-Lab is another tool used to automate survey/triage forensic inspections of computers in various kinds of investigations (http://www.adfsolutions.com). Another such tool, named "System for Triaging Key Evidence" (STRIKE), is a handheld device with a touch screen that automates survey/triage forensic inspections in the field (http://www.idealcorp.com). This tool can be programmed to recover and display deleted files of a particular kind, perform keyword searches in multiple languages, and automatically execute other basic forensic inspection tasks (Fig. 1). This approach is useful for checking computers for contraband at a border, or for verifying that probationers' or parolees' computers do not contain prohibited materials. In addition to increasing efficiency, automation can enable less skilled technicians to perform survey/triage tasks according to preprogrammed parameters, thus reducing the load on experienced forensic examiners. However, the results of such survey/triage inspection tools are not a substitute for forensic examination. If the survey/triage forensic inspection reveals that the computer contains potentially relevant digital evidence, the computer can be tagged for further levels of examination by an experienced forensic examiner.

The survey/triage approach is also effective for examining network traffic. A quick inspection of captured data may reveal sufficient evidence to break a case, showing the distribution of contraband or the theft of intellectual property. Tools such as NetIntercept (http://www.sandstorm.net) and NetWitness (http://www.netwitness.com) enable this type of inspection of network traffic, allowing digital investigators to view a gallery of images in captured network traffic as shown in Fig. 2.

Survey/triage forensic inspections have been used by forensic examiners in criminal and civil contexts for many years. However, there are no published guidelines for performing these inspections, leading to widely varying methods. Performing a keyword search of logical files may not be effective if evidence is in unallocated space or unsearchable files, or when encryption is used. Furthermore, survey/triage forensic inspections that focus on specific known artifacts of criminal activities commonly found in past cases may overlook evidence relating to the production of child pornography, or the use of new technologies to facilitate criminal activity. To mitigate the risk of relevant evidence being overlooked, there is a need for guidelines and continuously updated survey/triage forensic inspection tools to reduce the risk of missed evidence. In addition, forensic examiners must be trained to assess the results of a survey/triage forensic inspection, and decide if more resources are warranted for a particular situation.

Preliminary Forensic Examination

Items that have been identified as significant during a survey/triage forensic inspection generally require further forensic examination to extract useable evidence. However, digital investigators often need information quickly and cannot afford to wait for an in-depth forensic examination. The goal of a preliminary forensic examination is to provide investigators with information swiftly that will aide them in conducting interviews and developing leads. Whereas a survey/triage forensic inspection simply identifies potential evidence, a preliminary forensic examination interprets the



Total: 101
00:04:25
1 / 24

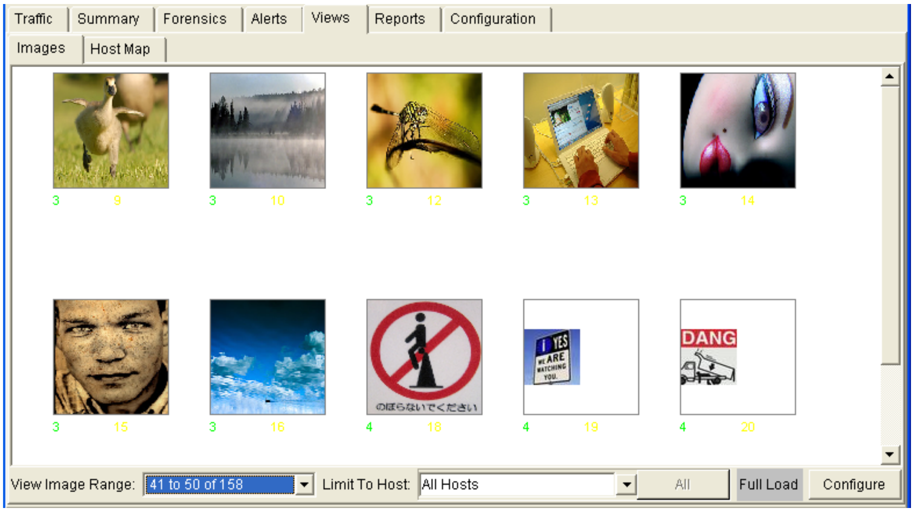
brndlog.txt
36%

index.dat
46%

waldo@travel.yahoo[2].txt
36%

61%
61%
61%
1 / 9

FIG. 1—*STRIKE screenshot showing text and image search for items with percentage likelihood of matching search criteria.*



3 9
3 10
3 12
3 13
3 14
3 15
3 16
4 18
4 19
4 20

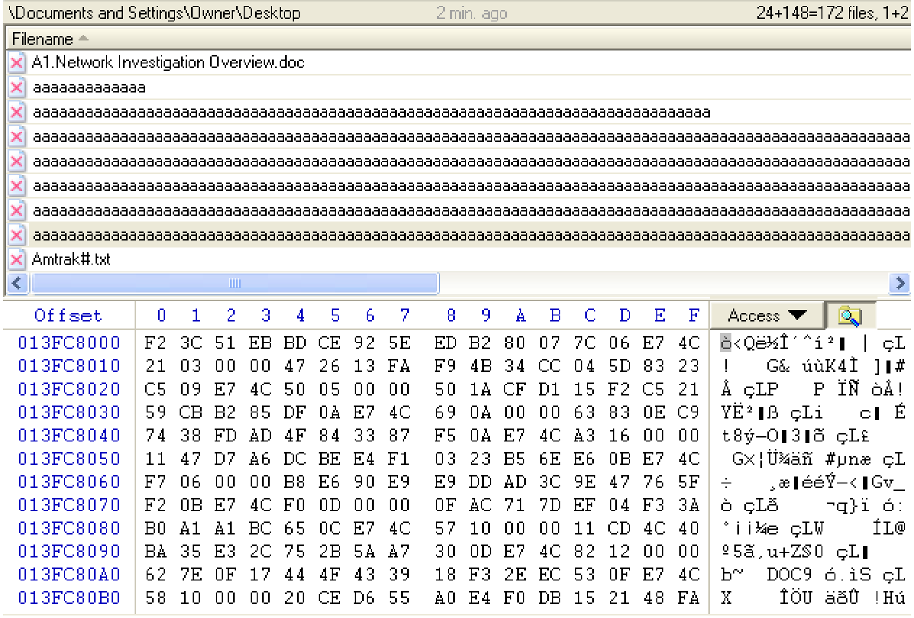
View Image Range: 41 to 50 of 158
Limit To Host: All Hosts

FIG. 2—*NetIntercept showing thumbnail views of graphics files captured network traffic.*

relevant evidence and makes it available in a form that is useful to others involved in the case. The results of a preliminary forensic examination can be sufficient to obtain a confession or admission and can even bring an investigation to a close without a more extensive forensic examination. Importantly, a preliminary forensic examination can be performed in read-only mode, eliminating the need to create forensic duplicates of all available sources of digital evidence. When a particularly important piece of evidence is located, appropriate forensic preservation steps can be performed if necessary.

In a 2005 case, a search warrant was conducted on a house of a known child pornographer, yielding four computers and a large amount of other digital media. Based on an experimental search protocol, forensic examiners were on scene to conduct write-blocked preliminary forensic examinations of the computers. While forensic examiners were unable to find contraband on the computers, they identified Microsoft Internet Explorer log files which showed the computer user accessing image files from the CD-ROM drive of the computer. Because the forensic examination was conducted on scene, this evidence was used by the investigators to confront the suspect. In the face of clear and convincing evidence showing that he accessed files with names like "8yo_preteen_sex.jpg" on his optical media drive, the defendant quickly confessed, and produced a CD with his entire collection of child pornography. Given the large cache of digital evidence seized from the house, it could have taken months or longer for investigators to identify this one CD as having contraband.

Unlike an in-depth forensic examination, a preliminary forensic examination does not delve into every place where evidence might be found. For example, when child pornography is found in active



```
\Documents and Settings\Owner\Desktop          2 min. ago          24+148=172 files, 1+2
Filename
A1.Network Investigation Overview.doc
aaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Amtrak#.txt

  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   Access
013FC8000   F2 3C 51 EB BD CE 92 5E  ED B2 80 07 7C 06 E7 4C   ò<Që½Î´^í²▌ | çL
013FC8010   21 03 00 00 47 26 13 FA  F9 4B 34 CC 04 5D 83 23   !   G& úùK4Ì ]▌#
013FC8020   C5 09 E7 4C 50 05 00 00  50 1A CF D1 15 F2 C5 21   Å çLP   P ÏÑ òÅ!
013FC8030   59 CB B2 85 DF 0A E7 4C  69 0A 00 00 63 83 0E C9   YË²▌ß çLi   c▌ É
013FC8040   74 38 FD AD 4F 84 33 87  F5 0A E7 4C A3 16 00 00   t8ý-O▌3▌õ çL£
013FC8050   11 47 D7 A6 DC BE E4 F1  03 23 B5 6E E6 0B E7 4C    G×¦Ü¾äñ #µnæ çL
013FC8060   F7 06 00 00 B8 E6 90 E9  E9 DD AD 3C 9E 47 76 5F   ÷   ¸æ▌ééÝ-<▌Gv_
013FC8070   F2 0B E7 4C F0 0D 00 00  0F AC 71 7D EF 04 F3 3A   ò çLð    ¬q}ï ó:
013FC8080   B0 A1 A1 BC 65 0C E7 4C  57 10 00 00 11 CD 4C 40   °¡¡¼e çLW    ÍL@
013FC8090   BA 35 E3 2C 75 2B 5A A7  30 0D E7 4C 82 12 00 00   º5ã,u+Z§0 çL▌
013FC80A0   62 7E 0F 17 44 4F 43 39  18 F3 2E EC 53 0F E7 4C   b~  DOC9 ó.ìS çL
013FC80B0   58 10 00 00 20 CE D6 55  A0 E4 F0 DB 15 21 48 FA   X    ÎÖU äðÛ !Hú
```

FIG. 3—*Traces of wiping activity observed using X-Ways Forensics software during a survey forensic examination of a hard drive may indicate that vital evidence has been destroyed.*

and recoverable deleted files, a preliminary forensic examination of user activities on the system such as Web browsing may provide sufficient corroborating evidence to show the defendant's intent to possess the contraband. More importantly, the information obtained from a preliminary forensic examination may identify an imminent threat and help investigators prevent further harm. For instance, a preliminary forensic examination may indicate that a murderer plans to kill again, or that a sexual predator has access to a child.

As another example of the usefulness of preliminary forensic examinations, when an individual travels to meet a "victim" that is really an undercover police officer, the investigator generally has incriminating log files and communications that form a strong case on their own. In such cases, forensic examiners could perform a preliminary forensic examination of the defendant's computer in read-only mode for evidence of the interactions with the online undercover operative. Even if copies of the investigator's interaction with the suspect are not found, a preliminary forensic examination may identify other victims, or, as often is the case, evidence of other crimes that can, and should be charged.

A preliminary forensic examination of available media can also show that attempts were made to destroy evidence using wiping or disk cleaning software as shown in Fig. 3. Such traces of destruction of evidence may alert forensic examiners of the need for more in-depth forensic examination to locate incriminating digital evidence.

An illustration of how a preliminary forensic examination could function in a child pornography possession investigation is as follows. Suppose that no forensic duplicate is created and a write-blocker is used to protect the original media. The forensic examiner can quickly extract the potential child pornography, document the files' characteristics and context (e.g., to show that the contraband was found in a folder named "Lolitas" as opposed to it being found in unallocated space) and extract the information to be delivered for proper validation, maintaining integrity checks and chain of custody along the way.

Also with regard to forensic examinations in child pornography cases, it can be efficacious to limit the number of files that will be used as evidence without the need for producing hundreds of thousands of images. Additionally, automated techniques can be used for identifying known images. If five images will support a conviction, there is little sense in extracting and individually examining 100,000 images. There is little chance that the prosecution will charge 100,000 counts of possession, although some of the files may be quickly identified by hash-matching of previously identified/adjudicated images. It is far more prudent to perform a preliminary forensic examination to identify files that can easily be proven to have been viewed and thus "knowingly possessed" by the offender. Files with this type of corroborating evidence can promptly be extracted for use in prosecution, foregoing the voluminous production and examination of extraneous images.

In the United States, the National Center for Missing and Exploited Children, Exploited Child Division houses the Child Victim Identification Project. The Exploited Child Unit amasses hash values of images depicting known victims.[1] In the United Kingdom, the Exploitation and Online Protection (CEOP) Center produces similar hash sets that are used internally with their Child-Base image-recognition software, and that are provided to Interpol (http://ceop.gov.uk/). In this context, "known" means that law enforcement authorities can attest to the child's existence and the authenticity of the image. Known images versus suspected images are then documented and the final report prepared. Hash values of known images can be used in a preliminary forensic examination to expedite this type of analysis.[2]

Of course, when performing a preliminary forensic examination, there is a risk that relevant evidence will be missed in an attempt to expedite the forensic process. For instance, the risk of searching

[1] An online pamphlet describing the program is available from the NCMEC (23). The Internet Watch Foundation (http://www.iwf.org.uk) works closely with NCMEC. In Ireland, COPINE (http://www.copine.ie) maintained a similar database until Interpol took it over. Interpol is currently in the process of developing a G8 database for international use (24).

[2] http://www. internationalresourcecentre.org under "Victim Identification" (last accessed 5/30/08).

only for known files is that homemade and altered images may be overlooked. As previously mentioned, this risk can be mitigated by training forensic examiners to assess the results of a preliminary forensic examination, and decide whether a more in-depth forensic examination is required in any particular case.

In-depth Forensic Examination

Several situations require in-depth forensic examination of digital media. In-depth forensic examination is warranted when evidence destruction is suspected, when additional questions arise and when a case nears trial. When evidence destruction is suspected, an in-depth forensic examination is required to reconstruct the actions and to determine the method and intent. Documenting these actions may lead to additional criminal charges or sanctions.

When there are remaining questions after a preliminary forensic examination, an in-depth forensic examination is required. For example, a preliminary forensic examination may document communications regarding prostitution. An in-depth forensic examination would be warranted if money laundering and corrupt organization activities were also suspected.

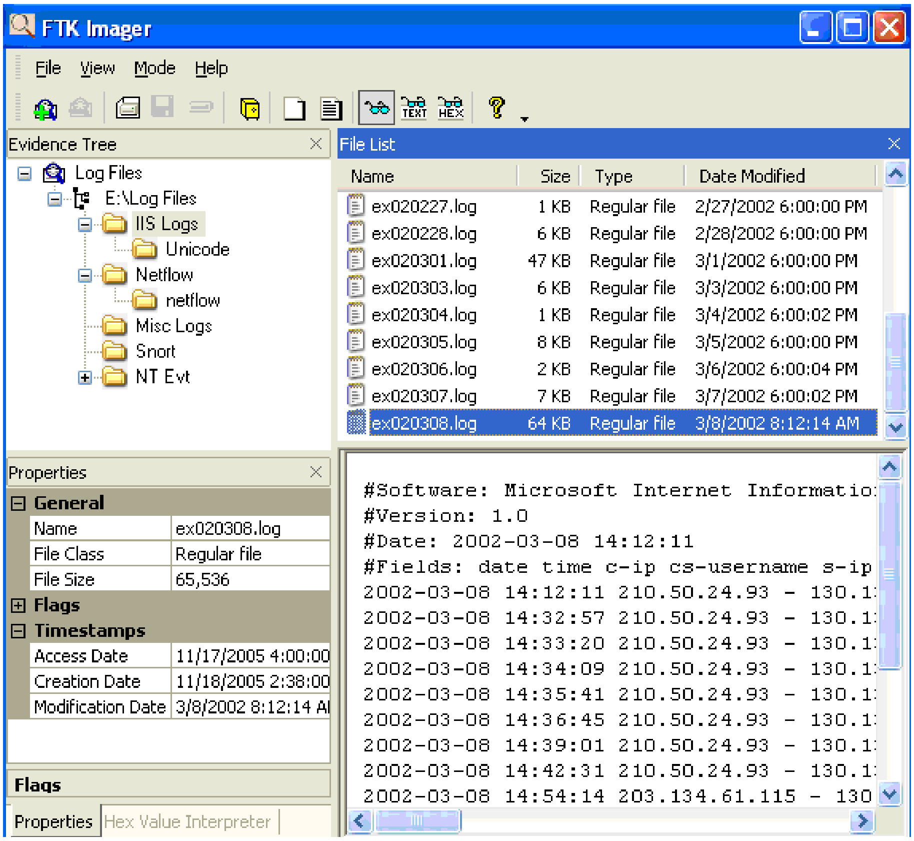
Finally, when a case is going to trial, a more in-depth forensic examination is generally required. For instance, if the defense claims that incriminating evidence was intentionally placed on the system via a Trojan Horse program, it may be necessary for forensic examiners to perform more extensive analysis to ascertain whether or not the computer was, in fact, infected with a virus or had the necessary vulnerabilities to allow such an attack. It should be noted however, that possession cases rarely involve such complexities as Trojan Horse programs or hacked computers and that it is a waste of resources to look for them in all cases.

In situations where an in-depth forensic examination is required, it is best practice to create a forensic duplicate of the original evidence since the evidence will be accessed repeatedly and extensive processing will generally have to be performed on the data. However, it may not be necessary to create a forensic duplicate of all data on the computer system as described in the next section.

Selective Forensic Preservation

There are situations in which it may not be desirable to create a forensic duplicate of the entire system. For instance, a server with terabytes of storage may only contain a small amount of relevant evidence. In one case, a forensic duplicate of an entire Exchange e-mail server was acquired when it was only necessary to extract a limited number of mailboxes of relevant custodians, turning a relatively straightforward preservation task into a costly effort. In another case, when confronted with an Oracle database, investigators proposed imaging all of the underlying servers when it was only necessary to extract a limited set of database records. In addition to being unnecessarily costly and disruptive to an organization's operations, the creation of forensic duplicates of such a database system makes it difficult to extract the desired data and may not preserve all of the relevant information such as archives on backup tapes and logs sent to a remote system. In such cases, taking the time to understand the computer systems involved and where relevant data resides for the time of interest can avoid unnecessary work and maximize the amount of relevant information that is preserved.

If only portions of evidentiary media must be forensically preserved, selective preservation may be feasible. This enables in-depth forensic examination of the relevant digital evidence without



Name	Size	Type	Date Modified
ex020227.log	1 KB	Regular file	2/27/2002 6:00:00 PM
ex020228.log	6 KB	Regular file	2/28/2002 6:00:00 PM
ex020301.log	47 KB	Regular file	3/1/2002 6:00:00 PM
ex020303.log	6 KB	Regular file	3/3/2002 6:00:00 PM
ex020304.log	1 KB	Regular file	3/4/2002 6:00:02 PM
ex020305.log	8 KB	Regular file	3/5/2002 6:00:00 PM
ex020306.log	2 KB	Regular file	3/6/2002 6:00:04 PM
ex020307.log	7 KB	Regular file	3/7/2002 6:00:02 PM
ex020308.log	64 KB	Regular file	3/8/2002 8:12:14 AM

General	
Name	ex020308.log
File Class	Regular file
File Size	65,536
Flags	
Timestamps	
Access Date	11/17/2005 4:00:00
Creation Date	11/18/2005 2:38:00
Modification Date	3/8/2002 8:12:14 A

```
#Software: Microsoft Internet Informatio
#Version: 1.0
#Date: 2002-03-08 14:12:11
#Fields: date time c-ip cs-username s-ip
2002-03-08 14:12:11 210.50.24.93 - 130.1
2002-03-08 14:32:57 210.50.24.93 - 130.1
2002-03-08 14:33:20 210.50.24.93 - 130.1
2002-03-08 14:34:09 210.50.24.93 - 130.1
2002-03-08 14:35:41 210.50.24.93 - 130.1
2002-03-08 14:36:45 210.50.24.93 - 130.1
2002-03-08 14:39:01 210.50.24.93 - 130.1
2002-03-08 14:42:31 210.50.24.93 - 130.1
2002-03-08 14:54:14 203.134.61.115 - 130
```

FIG. 4—*FTK Imager being used to preserve a folder containing various log files.*

duplicating the entire system. Selective preservation can be performed while satisfying forensic requirements of authenticity and integrity. Figure 4 shows FTK Imager being used to preserve a folder containing various log files in a forensically sound manner (http://www.accessdata.com). EnCase also has the capability to perform a selective preservation, called a ''Logical Evidence File'' (http://www.guidancesoftware.com). To provide additional functionality, a more comprehensive approach to selective forensic preservation of digital evidence has been developed (16).

Examples of Success

Survey/triage forensic inspections, preliminary forensic examinations, and selective preservation are already used in incident handling and civil discovery. For example, in a large-scale intrusion, the majority of systems may only contain a small amount of useful evidence, and indiscriminately imaging the hundreds of systems that were involved would be imprudent. Once relevant systems have been identified through survey/triage forensic inspections, it is generally sufficient to perform preliminary forensic examinations of most systems. Then, if there is a concern that the system in question contains additional useful data, the decision can be made to create a full forensic duplicate and perform an in-depth forensic examination. This approach permits a more thorough investigation with limited resources and results in more evidence from multiple independent sources.

One approach to performing survey/triage forensic inspections, preliminary forensic examinations, and selective preservation of volatile data or data from the hard drives without shutting down or imaging the entire system is to use a CD-ROM like Helix. Helix is specifically designed for this type of examination at the computer console and makes minimal changes to the system. The Helix live incident response user interface is shown in Fig. 5.

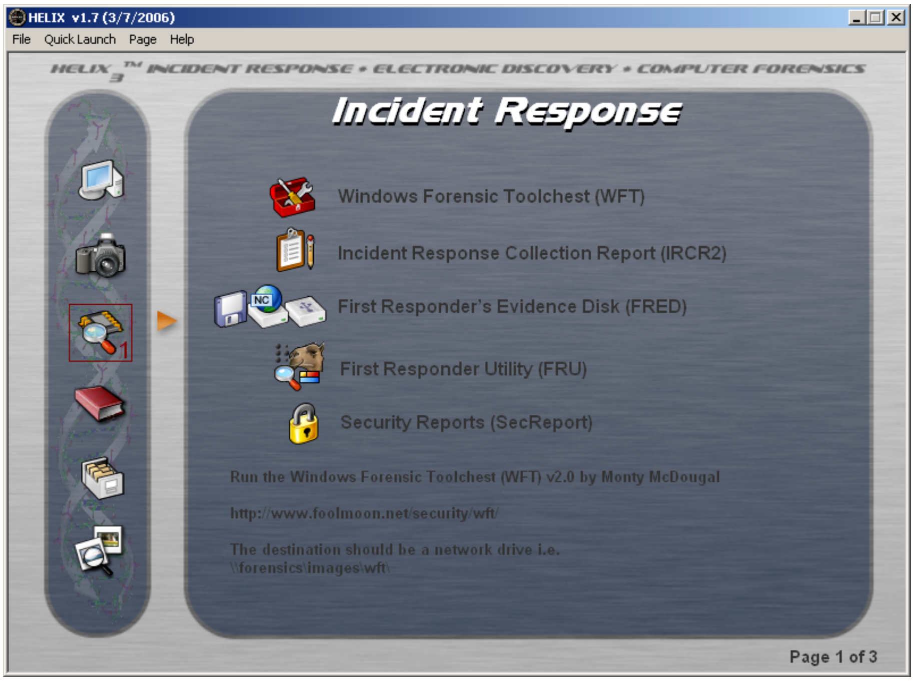
Several commercial tools have been developed to support remote live examinations in a forensically sound manner, including EnCase Enterprise Edition, F-Response (http://www.f-response.com), Online DFS (http://www.cyberstc.com), and ProDiscover IR (http://www.techpathways.com). These tools connect to the subject system via a network connection, providing a remote view of storage media and memory contents. These tools can be used to perform survey/triage forensic inspections of a large number of live computers on a network. In more complex cases, such as those involving sophisticated security breaches, investigators may need to use their knowledge of the offender's method of operation to create customized ''antidote'' programs that perform automated, remote survey/triage forensic inspections, searching all computers on a network to locate those that were targeted by the offender (17).

Remote forensic tools can also be used to perform preliminary forensic examinations and selective preservation of any evidence that is located on the remote systems. Figure 6 shows EnCase Enterprise being used to view a file on an encrypted disk on a remote computer. These tools can also be used to capture a forensic duplicate of the subject hard drive or other attached storage media should the need arise.

Provided care is taken to identify all relevant evidence on the live system, this approach is very efficient and is useful for processing a large number of systems. There is a risk that a rootkit could conceal useful information. Therefore, forensic examiners must be taught to identify such situations and take the necessary steps to preserve the relevant digital evidence.

Discussion

Although every crime or case theoretically should be addressed with the same rigor, it is not possible to do so in practice, given limited resources. If the DFL accepted all cases, there would be an unmanageable number of cases—a case that involves $100 sneakers, $15 lip liner, child pornography, or a $10 million securities fraud all competing for limited resources. Practices that accept every case that comes in when there are limited human resources

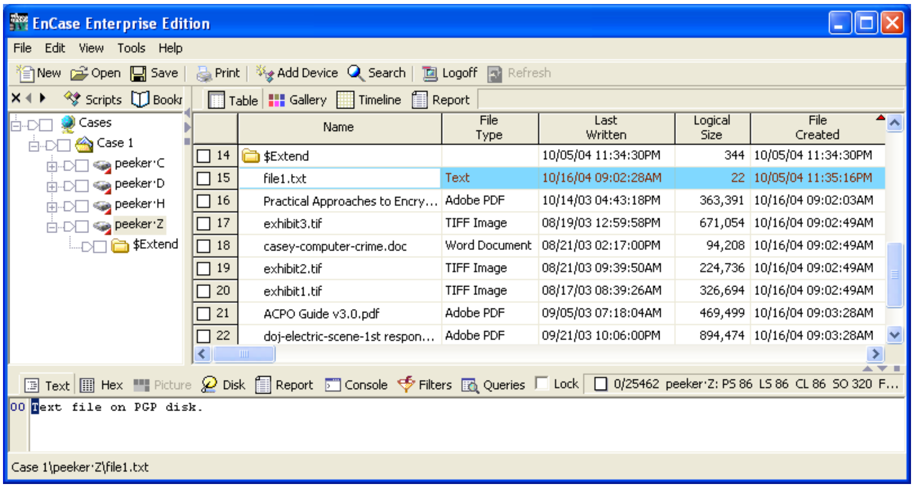

HELIX v1.7 (3/7/2006)
File
Quick Launch
Page
Help
HELIX3™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Incident Response
Windows Forensic Toolchest (WFT)
Incident Response Collection Report (IRCR2)
First Responder's Evidence Disk (FRED)
First Responder Utility (FRU)
Security Reports (SecReport)
1
Page 1 of 3

Run the Windows Forensic Toolchest (WFT) v2.0 by Monty McDougal

http://www.foolmoon.net/security/wft/

The destination should be a network drive i.e.
\\forensics\images\wft\

FIG. 5—*Windows Incident Response interface on Helix CD-ROM.*



	Name	File Type	Last Written	Logical Size	File Created
□ 14	$Extend		10/05/04 11:34:30PM	344	10/05/04 11:34:30PM
□ 15	file1.txt	Text	10/16/04 09:02:28AM	22	10/05/04 11:35:16PM
□ 16	Practical Approaches to Encry…	Adobe PDF	10/14/03 04:43:18PM	363,391	10/16/04 09:02:03AM
□ 17	exhibit3.tif	TIFF Image	08/19/03 12:59:58PM	671,054	10/16/04 09:02:49AM
□ 18	casey-computer-crime.doc	Word Document	08/21/03 02:17:00PM	94,208	10/16/04 09:02:49AM
□ 19	exhibit2.tif	TIFF Image	08/21/03 09:39:50AM	224,736	10/16/04 09:02:49AM
□ 20	exhibit1.tif	TIFF Image	08/17/03 08:39:26AM	326,694	10/16/04 09:02:49AM
□ 21	ACPO Guide v3.0.pdf	Adobe PDF	09/05/03 07:18:04AM	469,499	10/16/04 09:03:28AM
□ 22	doj-electric-scene-1st respon…	Adobe PDF	09/21/03 10:06:00PM	894,474	10/16/04 09:03:28AM

□ 0/25462 peeker'Z: PS 86 LS 86 CL 86 SO 320 F…

```
00 Text file on PGP disk.
```

Case 1\peeker'Z\file1.txt

FIG. 6—*EnCase Enterprise being used to view a file on an encrypted disk on a remote computer (18).*

to process the evidence set up the DFL for failure. DFLs must prioritize cases they receive in order to avoid overload and prolonged backlogs and, when deciding how many resources to expend on a particular case, a threshold is necessary. Many laboratories already set thresholds on the cases they accept, or only accept certain types of cases.

To ensure excellent "customer service" and to support justice and safety protection, DFLs must establish thresholds and protocols that facilitate the efforts of digital investigators, and educate their "customers" about their priorities and appropriate uses of their resources. DFLs can refine their protocols to address common types of cases and provide guidance for expediting the analysis. For example, a protocol for examining hard drives for child pornography could recommend that forensic examiners preview each drive and perform a survey/triage forensic inspection looking only for images and specific keywords. If nothing is found during the survey/triage forensic inspection, the protocol could direct examiners to report the negative results to the investigator, noting what they searched for and the limitations of such a focused inspection. The investigators may decide that certain items deserve further attention, in which case the protocol could recommend that a preliminary forensic examination be performed. In this way, in-depth forensic examinations may become the exception rather than the rule, and setting thresholds will help DFLs decide when additional resources are appropriate for a particular case or piece of evidence.

Considerations relevant to setting thresholds include the seriousness of the offense, case circumstances and type of evidence sought, likelihood of missing exculpatory evidence, and the importance of other data on the storage media. However, each DFL prioritizes case work using criteria that are unique to their environment and case work. The following sections discuss the primary considerations that go into setting thresholds and are not intended to be exhaustive. Other factors that dictate immediate attention are the age, type, and condition of storage media (damaged media and handheld devices are best duplicated quickly).

Seriousness of Offense

It is generally reasonable to expend more resources on felonies than on misdemeanors. Analogously, it is generally reasonable to expend more resources on cases with large monetary losses, property impact, or that have major impact on policy issues. Some labs might consider eliminating availability of forensic examinations for misdemeanor and minor offenses altogether. Where statutes of limitation are short or the value added to the case by a written report of findings is minimal in comparison to the resources expended, it may be best to forego the digital forensic examination altogether.

It might be helpful to think in terms of the difference between the amount of resources the government should expend on a murder investigation versus a petty theft. At this point in time, the reality is that the resources expended to examine digital evidence are nearly equivalent to the resources expended on a homicide investigation. In some cases, *more* time is spent on digital evidence examinations than investigating a homicide. Is that sort of expenditure worth it to the taxpayer—who foots the bill—for relatively minor crimes like larceny under $1000?

Generally, it is also reasonable to give crimes that severely injure people priority over those that cause damage to property. Publicly funded DFLs should set a threshold for monetary loss, recognizing that the amount sometimes cannot be determined without some forensic examination of the digital evidence. It may be necessary to make an informed estimate to determine whether the losses justify the cost of the investigation. Part of this assessment involves intangible losses such as privacy and safety so that we maintain sight of important values and are not solely driven by monetary or political considerations.

Case Circumstances and Type of Evidence Sought

Although it is rarely possible at the outset of an investigation to know specifically what to look for from the beginning, the circumstances of the case usually lead digital investigators to seek certain types of evidence. Therefore, it is customary for forensic examiners to receive instructions from investigators or attorneys that define what is being sought. Such instructions generally provide background information about the case along with a general description of what kinds of evidence to look for. These instructions are broader than the narrow requests for specific evidence used in some DFLs with large case loads.

An understanding of the case and the type of evidence sought to a large degree dictates the approach a forensic examiner will take. For example, in a child pornography possession case, the forensic examiner will be looking for images. In some cases, there is little reason to extend the examination beyond a quick preview and extraction of the contraband. Oftentimes, this is sufficient to obtain a confession. In other cases, however, it may be difficult or judiciously unwise to proceed with images that may have been found in unallocated space or temporary internet files. These instances may begin with a preliminary forensic examination and, based on the results, lead to a more in-depth forensic examination to document a suspect's predilection and proclivity or in order to impeach his prior statements.

If during a preliminary forensic examination for possession, clues of more serious crimes are discovered, such as the possibility of local victims and the actual production of child pornography, the examination can be elevated according to the seriousness of the new evidence (keeping in mind that a new search warrant may be required).

If a target was suspected of possessing a large number of illegal images but none were found on his computer, this may be another indicator that further forensic examination is warranted. In this situation, the lower levels of forensic examination would result in a false-negative identification if the suspect has employed stegonography, encryption, or other countermeasures. It may be that the suspect's collection is stored on a completely different piece of media. On a case-by-case basis, the decision should be made whether or not to submit the evidence for more extensive forensic examination. Keep in mind however, the results of a more extensive examination may or may not be of any value. Some countermeasures are sophisticated enough to make it impossible for even the most thorough forensic examinations to unmask hidden data.

Fraud investigations, such as auction fraud or phishing, can complicate the threshold setting process because the scale of the crime may not be known initially and it may not be clear what types of evidence should be sought. To resolve doubts, it may be necessary to perform a preliminary forensic examination to provide the investigator with sufficient evidence to assess the extent of the criminal activities.

The role the evidence plays in the case should also be considered when planning the forensic examination. When digital evidence *is* the case, such as child pornography possession, some examination is required, such as a read-only preview of the original media to perform a survey/triage forensic inspection. However, if investigators already have strong evidence linking the suspect to the crime such as in an auction fraud or undercover sting operation, and simply want corroborating digital evidence, the DFL may decide that they do not have sufficient resources to accommodate any level of examination.

Ultimately, every case is unique and decisions about what digital evidence deserves further attention or what leads to pursue rely heavily on the discretion of the forensic examiner. This discretion underscores the necessity of proper training and the importance of forensic examiners, investigators and attorneys working closely together to make the most effective use of digital evidence.

Relevance of Other Digital Evidence

Part of setting thresholds involves assessing the likelihood of missing evidence that undermines the prosecution case or strengthens that of the defense. This concern is exacerbated by recent cases involving digital evidence. In the case of Julie Amero, the prosecution relied heavily on the presence of pornography on the hard drive of a classroom computer, ignoring Amero's claims that the images were placed there by a malicious Web site that was accessed inadvertently (19). Simon Bunce was arrested during Operation Ore for alleged access to child pornography, despite the fact that someone else had subscribed to the Web sites in question, used his stolen credit card, and forensic examiners did not find any child pornography on his computer (20).

To prevent such problems, DFLs need to evaluate the veracity of the evidence to determine whether further forensic examination is required. When a critical issue in a case remains unanswered, investigators and attorneys must decide whether further forensic examination is needed or the case is too weak to proceed. For instance, when records from servers on the Internet suggest that a person downloaded child pornography but none is found on his computer and associated storage media during a survey/triage forensic inspection, at the very least a preliminary forensic examination is required. Alternately, if a preliminary forensic examination of a computer yields sufficient evidence but the defendant claims that a malicious hack or a Trojan Horse program was used to remotely control his computer by some nefarious individual, then it may be necessary to perform an in-depth forensic examination to ascertain whether or not the computer was, in fact, infected with a virus or had the necessary vulnerabilities to allow such an attack.

Arguably, it is not possible to examine every byte on a hard drive individually, so there is always a risk of missing something. However, if a case is so weak that it could be undermined by a relatively small amount of digital evidence, it probably will not make it to court. Even if such a case does make it to court, there is a slim likelihood that it will result in conviction—nor should it. Obviously, if the case is not heading for court or a conviction, the wisdom of investing public funds in the endeavor is dubious.

Given the opportunity, a competent forensic examiner can assist investigators and prosecutors in understanding digital evidence and its limitations. Again, this demonstrates the need for close collaboration between, and proper training of, forensic examiners, investigators and attorneys.

When a case makes it to trial in the United Kingdom, there are disclosure requirements that must be considered to ensure that all relevant material is available to the accused. The principle of disclosure is that "a fair trial consists of an examination not just of all the evidence the parties wish to rely on but also all other relevant subject matter" (21). At the same time, there are protections against unreasonably broad requests for disclosure such as irrelevant material and "spurious applications or arguments which serve to divert the trial process from examining the real issues before the court" (21). Existing DFL practices in the U.K. already take disclosure obligations into consideration and the approach described in this paper does not fundamentally change these practices. By retaining all original evidence that was collected in a case, DFLs can produce whatever is required when the case goes to trial. As always, forensic examiners are generally advised to document their actions and any discussion with an investigator or prosecutor regarding specific avenues of inquiry, and they should be prepared to disclose their documentation and justify their actions when required.

Ethical Considerations

Cybercrime presents new and unique challenges, but the ethical challenges that forensic examinations of digital evidence presents are really not very different from ethical questions that have faced generations of law enforcement administrators and forensic scientists.

Deciding whether to take a case and what level of resources to allocate to each forensic examination are difficult decisions. What if evidence of other victims is overlooked because an in-depth forensic examination was not performed in a child pornography possession case? What if there is a murder on video and you miss it? Every day, police officers and law enforcement administrators decide how much is enough—how much evidence is enough to prove the case against the accused? How much investigation is enough to "solve" a case? It is their job to make these decisions, and determine what amount of time and expenditure is reasonable in each case. They decide how many witnesses should be interviewed. Together with the prosecutor, they decide how many charges to bring against a particular defendant.

To assist DFLs in setting thresholds, it is important to establish their ethical duty. As forensic scientists, examiners of digital evidence should be neutral. That principle is fundamental. Whether instructed by the prosecution or defense, forensic examiners have a duty to process digital evidence according to the instructions provided to the best of their abilities. Forensic examiners cannot ignore details that weaken the prosecution case or may assist the defense. Utilizing thresholds to prioritize cases and manage resources does not facilitate ignorance of potentially exculpatory evidence. When forensic examiners discover potentially exculpatory evidence, at that point, they have an ethical and legal obligation to disclose the exculpatory information. When forensic examiners are provided with an alternative explanation offered by the defendant, they have a duty to test such defense claims thoroughly. However, there is no ethical requirement that the forensic examiner fully investigate any or all potential defenses. To do so is generally impractical.

Currently, DFLs are setting thresholds informally and make ad hoc decisions about what level of forensic examination is necessary, but, because the process is informal, it tends to be subjective and undocumented. DFL administrators tend to err on the side of caution, and due to their cautionary approach, delay results. Our thesis is that "investigation delayed is justice denied." In addition to harming defendants, delays in processing digital evidence result in lost opportunities to apprehend and prosecute other criminals and protect public safety.

It is imperative that we start to hone our processes and focus on cost and time efficiency in digital forensics. In so doing, we must develop acceptable guidance for laboratories to define thresholds, and make more effective use of limited resources. At the very least, administrators should begin to document the factors they consider when accepting cases for examination and deciding the scope of examination. Tracking the hours spent on different types of cases and the amounts of data involved can help DFLs determine whether they are making effective use of resources. In addition, DFLs can obtain useful information from "customers" to determine whether their needs are being satisfied.

Ultimately, the aim should be to develop guidelines for performing threshold assessments and tailoring forensic examinations accordingly. By developing generally accepted guidelines, we can increase consistency across jurisdictions and set realistic expectations.

Conclusion

Forensic examination of digital evidence is an emerging field. Practitioners have been preoccupied with Herculean efforts to keep up with mounting case loads and to stay current with technological developments. The time has come to update our methods to deal with the mounting quantities of digital evidence, and to avoid causing harmful delays in the criminal justice process. DFLs can address these problems by establishing thresholds to prioritize cases and scaling the forensic examination process to fit the needs of the case. The scale of the examination should be dependent upon considerations that include the seriousness of the offense under investigation and the type of evidence sought.

Training investigators, forensic examiners, and prosecutors to recognize when a survey/triage forensic inspection or preliminary forensic examination are appropriate will maximize the investigative opportunities that digital evidence can create when it is available. Furthermore, by evaluating each case against the aforementioned thresholds prior to performing an in-depth forensic examination, DFLs can make more effective use of resources, satisfy the needs of more customers, and better support safety and justice.

Ethical considerations are difficult, but must be addressed head-on. Missed evidence is a concern with survey/triage forensic inspections and preliminary forensic examinations. The possibility of overlooking exculpatory evidence presents an ethical quandary for some (22). Forensic examiners must respond to all inquiries objectively, and they have a duty to report any potentially exculpatory or additional inculpatory evidence they find. Forensic examiners are also obliged to reevaluate their findings in light of defense statements. However, there is no ethical requirement that the forensic examiner fully investigate any or all potential defenses.

If DFLs are to keep up with mounting case loads while at the same time keeping current with technology developments, we must innovate and adapt to a constantly evolving field. Practical considerations that impede thresholds being implemented and procedures being streamlined include resistance on the part of practitioners, attorneys, and accrediting bodies. The authors' suggestion is to implement time-saving innovations and document them rather than wait for external forces to permit change. From that documentation, DFLs could consider collaborating to develop guidelines for establishing thresholds and performing each level of forensic examination. Collaboration could take the form of a committee or subcommittee of an existing accreditation organization, or formation of a new entity drawing from the digital evidence forensic community.

Acknowledgments

We thank Peter Sommer for his insight into the survey/triage process, duty of experts, and legal concerns in the United Kingdom. Thanks to Dr. James Casey for helping to hone and strengthen this paper.

References

1. Brown C, Kenneally E. Risk sensitive digital evidence collection. Digital Invest 2005;2(2):101–19.
2. Association of Chief Police Officers. Good practice guide for computer-based electronic evidence. London: ACPO, 2007, http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.
3. Standard Working Group on Digital Evidence. SWGDE best practices for computer forensics, Version 2.1 (July 2006). Florida: SWGDE, 2006, http://www.swgde.org/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf.
4. Reith M, Carr C, Gunsch G. An examination of digital forensic models. Int J Digital Evidence Fall 2002;1(3):10–22.
5. Rogers KM, Goldman J, Mislan R, Wedge T, Debrota S. Computer forensics field triage process model. Proceedings of the First Conference on Digital Forensics, Security and Law; 2006, http://www.digitalforensics-conference.org/CFFTPM/CDFSL-proceedings2006- CFFTPM.pdf.
6. Casey E. Digital evidence and computer crime: forensic science, computers, and the internet, 2nd rev. ed. London: Academic Press, 2004.
7. United States Department of Justice. Forensic examination of digital evidence: a guide for law enforcement. Washington DC: National Institute of Justice, 2004, http://www.ncjrs.gov/pdffiles1/nij/199408.pdf.
8. http://www.grayzone.com/may2003busts.htm (last accessed Aug. 20, 2008).
9. Carrier B, Spafford EH. Getting physical with the digital investigation process. Int J Digital Evidence 2003;2(2):2–21. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2003-29.pdf.

10. Risley S. Teachers want computer returned. Waterbury Republican-American 2005.
11. United States *v*. Brunette, 76 F. Supp. 2d 30 (D. Me. 1999), aff'd, 256 F.3d14 (1st Cir. 2001).
12. United States v Hernandez, 183 F, Supp. 2d 468 (D.F.R. 2002).
13. United States *v*. Triumph Capital Group (211 F.R.D. 31 D.Conn. 2002).
14. United States *v*. Syphers, 296 F. Supp. 2d 50, 55–56 (D.N.H. 2003).
15. Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. Digital Invest 2005;2(2):146–66.
16. Turner P. Selective and intelligent imaging using digital evidence bags. Proceedings of the Sixth Digital Forensic Research Workshop; 2006 Aug 14–16; London: Digital Invest3(S1):59–64, http://www.dfrws.org/2006/proceedings/8-Turner.pdf.
17. Casey E. Investigating sophisticated security breaches. Commun ACM 2006;49(2):48–55.
18. Casey E, Stanley A. Tool review—remote forensic preservation and examination tools. Digital Invest 2004;1(4):284–97.
19. Washkuch F. Judge grants Amero new trial in school-porn case. SC Mag 2007, http://www.scmagazineus.com/Judge-grants-Amero-new-trial-in-school-porn-case/article/35080/.
20. Sigsworth M. I was falsely branded a paedophile. BBC 2008, http://news.bbc.co.uk/1/hi/magazine/7326736.stm.
21. United Kingdom Attorney General's Office. Attorney General's guidelines on disclosure. London: UKAG, 2005, http://www.attorneygeneral.gov.uk/attachments/disclosure.doc.
22. Mario JR. A review of Anglo-American forensic professional codes of ethics with considerations for code design. Forensic Sci Int 2002;3(2–3):103–12.
23. http://www.missingkids.com/en_US/publications/NC166.pdf (last accessed Mar. 27, 2008).
24. http://www.internationalresourcecentre.org/missingkids/servlet/PageServlet?LanguageCountry=en_X2&PageId=2459 (last accessed May 30, 2008).

Additional information and reprint requests:
Eoghan Casey, M.A.
Johns Hopkins University Information Security Institute
3400 North Charles Street
4th Floor, Wyman Park Building
Baltimore, MD 21218
E-mail: eoghan@jhu.edu